

# 雲端服務環境之註冊表隱藏型Rootkit偵測機制研究

曾淑婷、曹偉駿

E-mail: 387218@mail.dyu.edu.tw

## 摘要

有鑑於Google、微軟、亞馬遜、IBM、戴爾、昇陽、惠普等國際大廠，皆大舉跨入雲端運算領域，其採用雲端多方面的應用與虛擬化技術，為PC領域帶來更好的桌面和軟體使用的體驗。因此，潛藏於雲端的應用虛擬化惡意軟體，尤其是間諜軟體和Rootkit，也成為了電腦安全領域重點防範的對象。從惡意程式的發展來看，具備一定程度的隱藏功能已經成為一種趨勢。在Windows系統下，惡意程式的存在和運行大都離不開系統登錄中的相關資訊，而惡意程式也常常隱藏於註冊表，故不可能真正刪除它們。因此，如何有效地偵測出隱藏於註冊表內的Rootkit，也就顯得格外重要。雖然有知名偵測軟體亦能偵測出隱藏於註冊表內的Rootkit，但面對新型Rootkit時，卻常常無法有效偵測。本研究為了偵測通過篡改註冊表檔而隱藏於作業系統的Rootkit，我們分析了常見的Rootkit 註冊表隱藏技術以及相關的偵測技術。在分析註冊表檔的格式以及註冊表操作控制流程後，本研究設計出一種新型的註冊表隱藏型Rootkit以及Rootkit偵測方式。通過虛擬化註冊表以及Win32系統底層註冊表鍵值的流程，獲取真實有效的註冊表鍵，能夠有效偵測出隱藏於雲端環境的Rootkit。

關鍵詞：雲端服務、惡意軟體、Rootkit、虛擬化註冊表、Windows作業系統

## 目錄

中文摘要	iii	英文摘要	iv
致謝詞	vi	內容目錄	vii
表目錄	ix	圖目錄	x
第一章 緒論	1	第一節 研究背景	1
第二章 研究動機與目的	2	第二節 研究限制	2
第三章 研究限制	3	第三節 研究流程	3
第四章 研究流程	3	第四節 研究限制	3
第五章 論文架構	5	第五節 論文架構	5
第二章 文獻探討	6	第一節 雲端虛擬化註冊表	6
第一節 雲端虛擬化註冊表	6	第二節 Rootkit惡意軟體	6
第二節 Rootkit惡意軟體	10	第三節 基於註冊表的Rootkit隱藏技術	12
第三節 基於註冊表的Rootkit隱藏技術	12	第四節 基於註冊表的Rootkit偵測技術	13
第四節 基於註冊表的Rootkit偵測技術	13	第三章 建構基於Windows雲端之註冊表型 Rootkit偵測機制	20
第三章 建構基於Windows雲端之註冊表型 Rootkit偵測機制	20	第一節 整體Rootkit偵測架構	20
第一節 整體Rootkit偵測架構	20	第二節 偵測機制	21
第二節 偵測機制	25	第三節 機制模組設計	25
第三節 機制模組設計	25	第四章 實驗設計與分析	29
第四章 實驗設計與分析	29	第一節 實驗環境	29
第一節 實驗環境	29	第二節 偵測機制測試	29
第二節 偵測機制測試	32	第三節 偵測能力與分析	32
第三節 偵測能力與分析	32	第五章 結論	37
第五章 結論	37	參考文獻	38
參考文獻	38		

## 參考文獻

- [1] S. Gold, "Protecting the cloud: attack vectors and other exploits," Network Security, no. 12, pp. 10-12, 2010.
- [2] D. Molina, M. Zimmerman, G. Roberts, M. Eadie and G. Peterson, "Timely Rootkit Detection During Live Response," Proceedings of IFIP International Federation for Information Processing, vol. 285, pp. 139-148, 2008.
- [3] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis and A. Vakali, "Cloud computing: Distributed Internet computing for IT and scientific research," Internet Computing, IEEE, vol. 13, no. 5, pp. 10-13, 2009.
- [4] 任雲韜, 李毅超, 曹躍, "基於註冊表Hive檔案的惡意程序隱藏檢測方法," 電子科技大學學報, vol. 36, no. 3, pp. 621-624, 2007.
- [5] 李冠儀, "以Windows Registry 為基礎之使用者行為異常偵測方法," 中央大學資訊管理學系學位論文, pp. 1-54, 2006.
- [6] 李偉斌, 王華勇, 羅平, "通過註冊表監控實現木馬檢測," 計算機工程與設計, vol. 27, no. 12, pp. 2220-2222, 2006.
- [7] 李錦, "Rootkit 木馬的隱藏機理與檢測技術剖析," 遼寧師範大學學報: 自然科學版, vol. 6, no. 2, pp. 176-178, 2009.
- [8] D. J. Farmer, "A Windows Registry Quick- Reference for the Everyday Examiner," pp. 1-14, 2007.
- [9] 楊彥, 黃皓, "Windows Rootkit 隱藏技術研究," 計算機工程, vol. 34, no. 12, pp. 152-156, 2008.
- [10] 劉?, 張家旺, "Rootkit 木馬隱藏技術分析與檢測技術綜述," 資訊安全與通信保密, no. 11, pp. 61-65, 2010.
- [11] 陳啟川, "惡意程式的隱形鬥篷 - Rootkit," Internet: <http://www.runpc.com.tw/content/content.aspx?id=103730> [May 18, 2013].
- [12] 蘇建郡, 方鵬喜, "Snort 於網站管理之應用," 第三屆離島資訊技術與應用研討會, pp. 334-340, 2003.

- [13] 申文迪, 羅克露, “輕量級虛擬機系統資源保護層研究,” 計算機工程, vol. 36, no. 14, pp. 127-128, 2010.
- [14] 王繼偉, 王嘉偉, 許家維, 謝續平, “基於虛擬機器外部觀察與映像檔比對的惡意程式分析,” 第二十屆資訊安全會議, pp. 69-74, 2010.
- [15] M. Christodorescu and S. Jha, “Testing Malware Detectors,” Proceedings of the ACM SIGSOFT international symposium on Software testing and analysis, vol. 29, no. 4, pp. 34-44, 2004.
- [16] E. Kumar, “Battle with the Unseen- understanding Rootkits on Windows,” Proceedings of International Conference on the 9th (AVAR), pp.82-97, 2006.
- [17] 張登銀, 高德華, 李鵬, “一種新的註冊表隱藏Rootkit 檢測方案,” 江蘇大學學報: 自然科學版, vol. 31, no. 3, pp. 328-333, 2010.
- [18] W. J. Tsaur, S. R. Wu and J. X. Wu, “Windows Rootkits Stealth Technologies in Cloud Computing,” Proceedings of Cryptology and Information Security Conference (CISC), Taiwan, 2012.
- [19] J. Zhang, S. Liu, J. Peng and A. Guan, “Techniques of User-mode Detecting System Service Descriptor Table,” Proceedings of the 13th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 96-101, 2009.
- [20] R. James, Butler II, “Detecting Compromises of Core Subsystems and Kernel Functions in Windows NT/2000/XP,” M.S. thesis, University of Maryland, Baltimore County, 2002.
- [21] D. Fu, S. Zhou, and C. Cao, “A Windows Rootkit Detection Method Based on Cross-view,” Proceedings of International Conference on E-product E-service and E-entertainment (ICEEE), pp. 1-3, 2010.
- [22] A. Pauna, “Improved self Adaptive Honey pots Capable of Detecting Rootkit Malware,” Proceedings of the 9th International Conference on Communications (COMM), pp. 281-284, 2012.
- [23] Z. Lu, G. Gan and J. Jiang, “Analysis and research on hidden technology based on kernel-level Rootkit process,” Proceedings of International Conference on Internet Technology and Applications (iTAP), pp. 1-4, 2011.
- [24] W. J. Tsaur and Y. C. Chen, “Exploring Rootkit Detectors Vulnerabilities Using a New Windows Hidden Driver Based Rootkit,” Proceedings of International Conference on Social Computing (SocialCom), IEEE, pp. 842-848, 2010.
- [25] W. Q. Wang, Z. G. Wu and S. X. Li, “Perfect Solution of Windows Registry Concealment Detection,” Computer Engineering, vol. 38, no. 14, pp. 106-108, 2012.